

~~TOP SECRET DINAR~~
The Operations of the National Security Agency

Jan 1961

Louis W. Tordella

Mr. McNamara:

I plan to review briefly the two main missions of the National Security Agency and the Service Cryptologic Agencies, those of Communications Security and Signals Intelligence. I then want to say a few words about the research and development which supports them, the personnel and budgetary support they receive, to mention some recent significant results and, in conclusion, to take a very brief look at the immediate future.

Let us consider first Communications Security which you will recall is intended to prevent unauthorized persons or nations from gaining useful information from the communications of the United States. Another way of looking at Communications Security is to consider that it provides the United States codes and ciphers and the rules for their use. The United States makes extensive use of radio communications which include the communications of its Armed Forces, its representatives abroad and others. In addition, there are many and important wire communications, both within the continental United States and abroad which carry information that has to be kept secret. We are aware that interception of our radio communications is occurring, and I will say more about that later. We likewise suspect at times that our wire communications may be tapped. In addition to our message type communications we also must make secure some of

~~TOP SECRET DINAR~~

Approved for Release by
NSA on 06-15-2010,
EOIA Case # 60938

~~TOP SECRET DINAR~~

the newer types of communications, for example, the requirement for one computer to communicate with another one with important data, or the requirement for encoding telemetry information from some of our satellite vehicles.

The major step in fulfilling the National Security Agency's COMSEC mission is that of providing cryptographic security, which means that we must provide the principles, the requirements, and the materials these equipments use up to make the communications secure against the unauthorized listener. We likewise have the problem of prescribing the rules for the physical protection of the devices and materials used in communications security. These minimum safeguards are prescribed by the National Security Agency but they are enforced by the using Agency.

The first step in providing cryptographic security is that of devising a machine or a system which can resist cryptanalytic attack. The Director of the National Security Agency is charged with the responsibility of approving all cryptographic systems that are used to encipher classified matter. First there is made a preliminary technical analysis of a proposed system or a device which is done by collaboration between the communications security analysts and the signals intelligence cryptanalysts. There is a continual cross-fertilization of ideas and skills between them. Once a system or a usage is approved analysis must continue in order to be aware of any errors or faults that may

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

jeopardize further material carried in these systems. One of the very important aspects of cryptographic security is that of proper usage. Without proper usage even the finest piece of equipment or the most involved system will not give the required security. The National Security Agency is responsible to prescribe proper usage but it does not enforce its rules. Each using Agency must police the people who use our equipments. NSA prescribes the rules and evaluates the seriousness in any error in usage that is made.

Our Communications Security office likewise is directly concerned with what might be termed "product engineering" of COMSEC equipments, and works directly with the military services in their service testing. Once a piece of equipment is adjudged acceptable for use by U.S. communicators, the National Security Agency does centralized procurement of all equipments used by the military services and the Federal agencies on a reimbursable basis. In this manner, advantage can be taken of price reductions that come from the economies of centralized bulk procurement. In addition to the work of producing and then evaluating the use of equipments, NSA produces all of the keying or setting elements which are consumed to provide the real security of the cryptographic devices in use. Some of these variable keying elements are changed from message to message; others daily, weekly, monthly, or even every year or two.

~~TOP SECRET DINAR~~

~~TOP SECRET DINAH~~

I have here a chart which illustrates the magnitude of this operation and I will have available for your inspection later some actual samples of these items. I shall mention only a few of them here but I believe the figures themselves are rather impressive. Perhaps the biggest production job that we engage in is that of producing codes. You will note the size of the FY-61 and the planned FY-62 production. These codes are used for the most part in operations where the risk of loss is great and the requirement for security and simplicity is paramount. For example, they are carried in an airplane which might very well crash or be shot down and the code recovered. They might be issued to a front line unit or one on hazardous assignment. Further, they are simple and easy to use and their very simplicity limits the volume of traffic they can safely carry and still withstand analysis. Therefore they ^{must be} ~~are~~ supplanted regularly ^{and frequently}. Another important item is the production of rotors which is an extensive operation and a very expensive one, both from a standpoint of the materials consumed and of the personnel required to do the job. These are the heart of a major variety of our machine cryptographic devices. A third very important cryptographic production is that of the key cards which are used on devices which encipher teletype or voice communications from one point to a second. You get a better picture of the actual volume of this activity when you multiply the number of books by 50, the number of cards in each book. A card is used at each terminal each time the equipment

~~TOP SECRET DINAH~~

~~TOP SECRET DINAR~~

is reset or at the beginning of each cryptographic period or day. I present this chart to you, Mr. McNamara, only to give you an idea of the magnitude of the production job in which we must engage to support not only the Services but also the Federal and civil agencies.

The National Security Agency also has, and I ~~will~~ mention it only in passing, certain lesser COMSEC responsibilities for NATO and for the Southeast Asian Treaty Organization. I will omit the details, except to note that we provide a certain number of limited materials, carefully selected, and certain evaluations of systems that are proposed for NATO and SEATO use.

I shall summarize our COMSEC mission by a brief examination of the status of United States Communications Security. With respect to our strategic communications, that is, those long haul for high level communications, I note that we are in excellent shape. Some users object at times to the cost of some of the equipments but the requirements for security, ease of maintenance and set-up, and the large number of components required to guarantee their safety against cryptanalytic attack all contribute to their final cost. Production in quantity and centralized procurement help considerably to reduce the final price. With respect to what we might call tactical communications we have one deficiency toward which we are directing major research efforts. The requirements for a low-cost, light-weight, secure voice equipment which is usable over any wire or radio line with any other similar equip-

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

ment are at this time simply incompatible with one another. We can provide either a more expensive and more complex device or we have equipments which require special ^{wire or} radio links. I would note that there is an extensive research effort in this field of voice handling, for the United States and world-wide industry have a real monetary as well as scientific interest in this area. We follow closely and, as appropriate, assist in this research.

There is one major area of concern which I feel I should mention, this is the problem of ^{spurious} ~~spinners~~ short-range radiation of exploitable data. The enemy has to be as it were across the street, in the adjacent house, or in the next room. Obviously this problem is of concern to the State Department and to all users of equipment in fixed locations which are very easily capable of supporting an unfriendly laboratory - like attack on the cryptomachine in use. It is a serious problem but is not of immediate direct concern to many users. It is also a problem that involves a great number of equipments other than just cryptographic devices. For example, certain special kinds of electric typewriters, facsimile equipment, and certain electric punches likewise radiate plain text. It is a government-wide problem that is being tackled on a government-wide basis under a committee of technical personnel established by the United States Communications Security Board and chaired by the National Security Agency. We are already making some progress in this area.

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

I now turn to the second main mission of the National Security Agency and the other cryptographic agencies, that of Signals Intelligence. SIGINT is made up of both COMINT and ELINT. COMINT involves, you will recall, the production of information from communications which we term communications intelligence or COMINT. ELINT is electronics intelligence which involves the production of information from non-communications devices like radars, navigational beacons, etc. In WW II, as also in Korea, the United States and the Allies in general, found that beforehand knowledge was invaluable when it came to positioning their forces to meet enemy threat. It permitted us to make the most effective utilization of what were at times limited resources. In this age of jet aircraft, of nuclear weapons, and of ballistic missiles, the need of timely prior information becomes even greater. The intelligence community has observed that signals intelligence is almost the sole source of this type of early warning information.

As Admiral Frost already has mentioned, the National Security Agency exercises operational and technical control of the United States signals intelligence resources in order first, to provide the maximum effective utilization of these available resources; second, to provide accurate, timely information which is not available from any other source; and third, to distribute this information to appropriate intelligence authorities throughout the world. I think I can illustrate this whole operation

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

in a general way by reference to this chart. I will identify first some of the types of activity that are represented on the chart. The intelligence agencies here are those of the Armed Services and J-2, the State Department, CIA, FBI, and AEC who constitute the United States Intelligence Board already discussed. This block is the National Security Agency; the Service Cryptologic Agencies are those of the Army, Navy, and Air Force. ^{In a few minutes} I will say more about the field installations ~~in a few minutes~~ which represent the intercept or collection and the processing activities located throughout the world; field Commanders are those Commanders represented, for example, by the Commander of the Strategic Air Command, the Commander of the Pacific Fleet, European Commanders, and various Commanders throughout the world.

Briefly this is how the SIGINT operations flow. The intelligence community in response to requirements from field commanders, or foreseeing the need for certain items of information, places requirements on USIB. Those requirements which can be satisfied ^{from SIGINT} and many can be satisfied only by SIGINT, are compiled by USIB and placed upon the National Security Agency in the form of a COMINT requirements list and an ELINT requirements list. The National Security Agency evaluates the signals intelligence capabilities and needs in relation to all the requirements at hand, including those ~~needed~~ ^{own} for technical support to its continued functions, and tasks ^{each} ~~the~~ Service Cryptologic Agencies to fulfill certain

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

of them. In working with the Service Cryptologic Agencies the National Security Agency assists them in developing their plans and programs and coordinates the final results. The National Security Agency is also charged with combining all SIGINT budgets with its own, and with presenting and justifying these budgets in support of the cryptologic programs to the Secretary of Defense.

~~XX~~ Intercept to provide the raw materials required for processing is done at the cryptologic agency field activities which I shall discuss in a moment. Certain of the technical processing is also assigned to the field when there exists ^a ~~the~~ competence to do the job and the primary need for the end product to be delivered with minimum delay. I stress these twin aspects of competence in the processing unit and need on the part of the field commander - both have to be present. When they are, or when the National Security Agency can assist the field activity with knowledgeable personnel and training to establish this competence, those requirements of field commanders that can be, are satisfied on a 24-hour-per-day basis close to the point of collection without any unnecessary delay or the extensive communications involved in sending the material to Washington and back out again.

The signals intelligence produced at the National Security Agency is that for which the primary need exists in Washington, e.g., diplomatic materials, ^{for which} or there are so many claimants with the same need that centralized processing is economical and necessary, ^{where} or the technical nature and

~~TOP SECRET DINAR~~

~~TOP SECRET DINA~~*and analytic equipment*

requirements of the problem are such that the skills to do the job exist only at Fort Meade. The National Security Agency output is delivered simultaneously and directly both to the intelligence agency consumers and to appropriate field commanders. This chart illustrates the flow of requirements which might require the National Security Agency to utilize a substantial amount of resources and perhaps do reprogramming of its own or Service Cryptologic Agency resources. There is also provision in this system for a field commander to go directly to one of the field installations placing on it a requirement which he anticipates could be satisfied there or to communicate directly with the National Security Agency placing on it a short-term requirement which can be satisfied with minimum resources or a few hours of work, or from material already available. This chart then shows only the over-all flow of major requirements, I might call them deliberate requirements. I want to note again that the field commander can get immediate, direct support from field installations that have the capability of providing that support or from the National Security Agency when the support material is immediately available for delivery to him.

I have frequently used the term Cryptologic Agency field installations and I think it appropriate that we now take a look at the map of our world-wide deployment. First I note the color coding: red indicates major Army installations, blue the major Navy installations, and green

~~TOP SECRET DINA~~

~~TOP SECRET DINAR~~

the major Air Force installations. The larger circles indicate collection and/or processing sites involving up to several hundred officers and men and the smaller circles represent collection sites perhaps not more than half a dozen collection positions, or very limited processing effort. You will note that we are disposed as best we can about our targets of major interest. We have the limitations, obviously, of geography, of logistics, and there are certain desirable locations where it is just not possible to have a station because of the unfavorable or unstable political climate.




(b) (1)
 (b) (3)-50 USC 403
 (b) (3)-P.L. 86-36



The number of

collection sites is governed by the requirement to intercept signals where they are available; to be in a position to serve the local field commander; and thirdly, our practical experience has shown that with more than about

(b) (1)
 (b) (3)-P.L. 86-36

 in one station the antenna and the electrical facilities become overloaded. Hence we have more than one site in the two accessible areas of high signal density.

I have several times used the word position. I think it might now be helpful if we saw two typical positions. This first picture shows the simplest type of position, one that would be used for an operator to copy manual Morse signals. It has a typewriter, two receivers, a headset and,

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

if he working on voice intercept instead of manual Morse, he will use this tape recorder. This might be termed the standard and conventional intercept position of which we still have more than [] Let us con-

(b)(1)
(b)(3)-P.L. 86-36

trast this one momentarily with one of the most complicated types of intercept positions required to cope with a complex signal which is called [] Even in this picture

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

we cannot quite see the whole position but you will note a number of receivers, various monitoring and tuning aids, a computer-like device here called a diarizer, and special printers. Besides the printers used to reproduce one of the channels, you will note here a battery of recorders for permanent storage of the signals and their delivery to the National Security Agency for analysis and ^{possibly} decryption. This type of position is illustrative of the complexity of equipment required to handle today's more sophisticated signals. Besides our complex operations I must again mention that we still have large quantities of manual Morse and radio telephone from which important SIGINT is derived.

At this point, as the Admiral has already mentioned, I note again our

(b)(1)
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

[] But the point I wish to make here, Sir, is that our collection

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

resources and also our analytic resources are carefully dovetailed and carefully tailored so as to eliminate unnecessary duplication and to complement one another to the maximum. To this end we exchange technical personnel who are integrated within each other's analytic organizations and have regular and continuous exchange of raw traffic, technical information, and SIGINT end product.

But there are serious limitations. Though our world-wide intercept capability, which I have just described, permits the accumulation of a great deal of raw material, it falls far short of what we would like to achieve. [REDACTED]

[REDACTED]
[REDACTED] Many kinds of directional transmissions and communications of limited range are unavailable to us in our present dispositions. The amounts of this kind of communication are growing. In addition new types of communication are being developed [REDACTED]
[REDACTED]

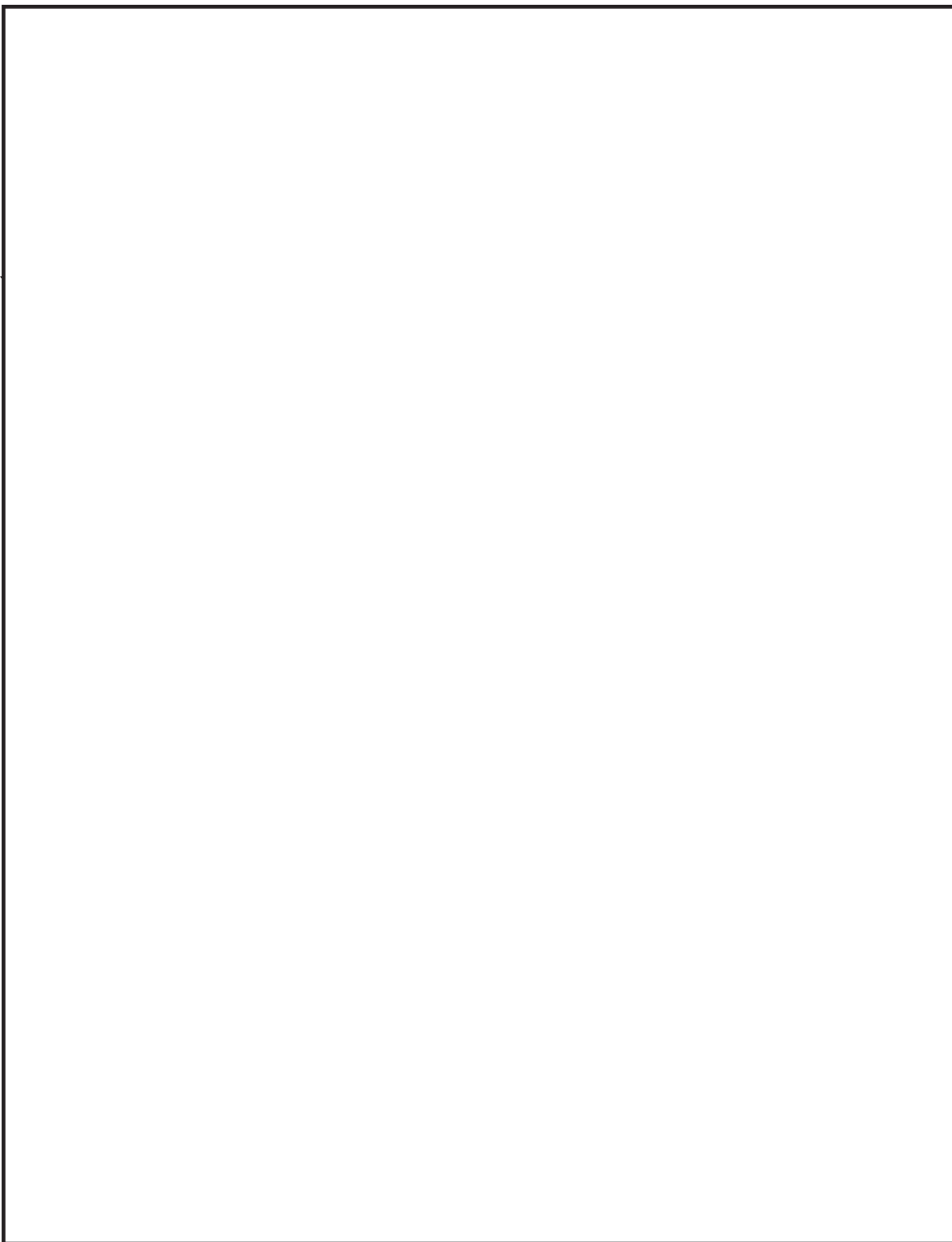
(b) (1)
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

Having spoken briefly as I did about the collection effort, I should like at this time to review in very general terms the status of our analytic effort for various areas throughout the world. First of all - our current major target - RUSSIA. [REDACTED]
[REDACTED]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~TOP SECRET DINAR~~

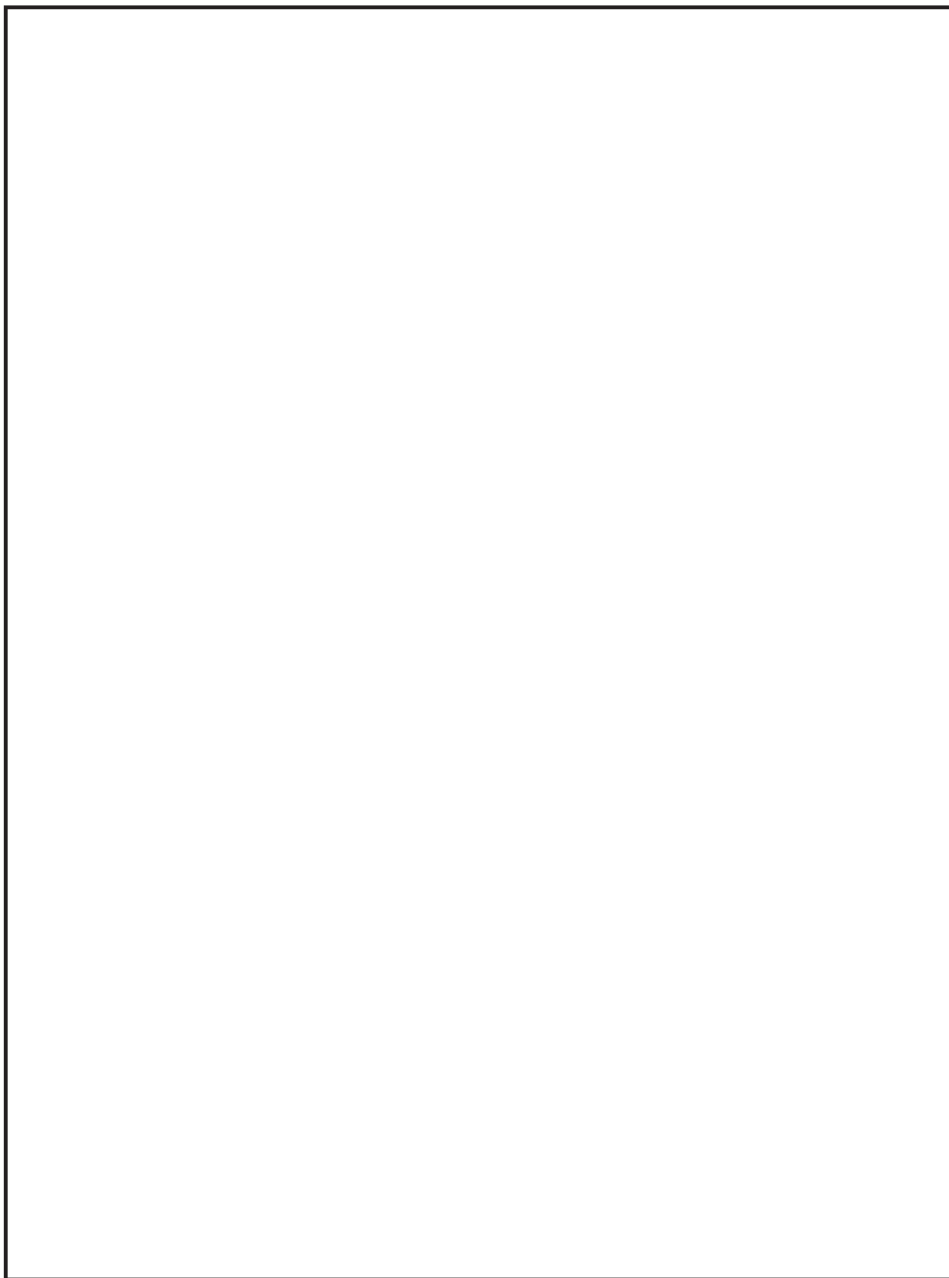
~~TOP SECRET DINAR~~



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

The net result of these technical accomplishments is the production of considerable intelligence from communications despite the attempts of the transmitting nations to deny us such information. As these nations improve their competence at concealment, we must step up our technical capability in our efforts to remain ahead. We are not always successful. It is consequently all the more disturbing that our successes have been publicly disclosed on several occasions, even before Martin and Mitchell. This publicity has stimulated communications security effort and has had the further result of tending to reduce the information carrying content of the communications we do intercept. We have read messages requiring important information to be transmitted over land lines only.

Signal Intelligence has traditionally been surrounded with an aura of extraordinary secrecy and has always been especially and carefully handled and transmitted. During the last war, the information derived from enemy communications was dubbed "Magic" by the British and the methods by which it was produced have been looked upon by "outsiders" as just short of this. Today our security problems are just as pressing and just as grave - perhaps even more so. It is rare, however, that the basic reason for the adoption of special security regulations for COMINT has been made clear. It is simply this. In no field of intelligence production can the enemy so easily deny us the material from which we derive our COMINT end product. In no endeavor does the United States stand to lose so much for so small a security breach.

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

These two major missions about which I have been talking, the communications security mission and the signals intelligence mission, are supported by an Office of Research and Development in the National Security Agency and also by Service research and developments programs. Over the years we have found that a strong research and development program is not only advantageous to us in that it enables prompt response to the ever-changing needs of COMSEC and SIGINT but it is absolutely necessary because of these reasons among others:

First, there is no commercial or university source of communications security or cryptanalytic skills which we can tap.

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

The field of cryptanalysis is a technical discipline of substantial breadth and difficulty comparable in complexity and scope to at least Masters level of work in Science for our better personnel. There is no such talent or capability outside the cryptologic field of the Government and we have therefore the problem of developing and extending this competence and training and training its practitioners.

Secondly, [REDACTED]

(b)(1)
(b)(3)-P.L. 86-36

[REDACTED] We therefore have to discover how to reconstruct these equipments using mathematical and electronics analysis techniques, then fabricate the equivalent to intercept the material.

Thirdly, we have very extensive requirements for high speed analytic equipments, usually more complex than modern computers. We also make very special applications of the most modern and complex conventional computers. The skills needed to do this logical design and to oversee the reduction of the design to workable electronic "super-computers", if I may use the term, is available nowhere except in the National Security Agency or in our sister organization in the United Kingdom and possibly also in Russia.

~~TOP SECRET DINAR~~

~~TOP SECRET DINA~~

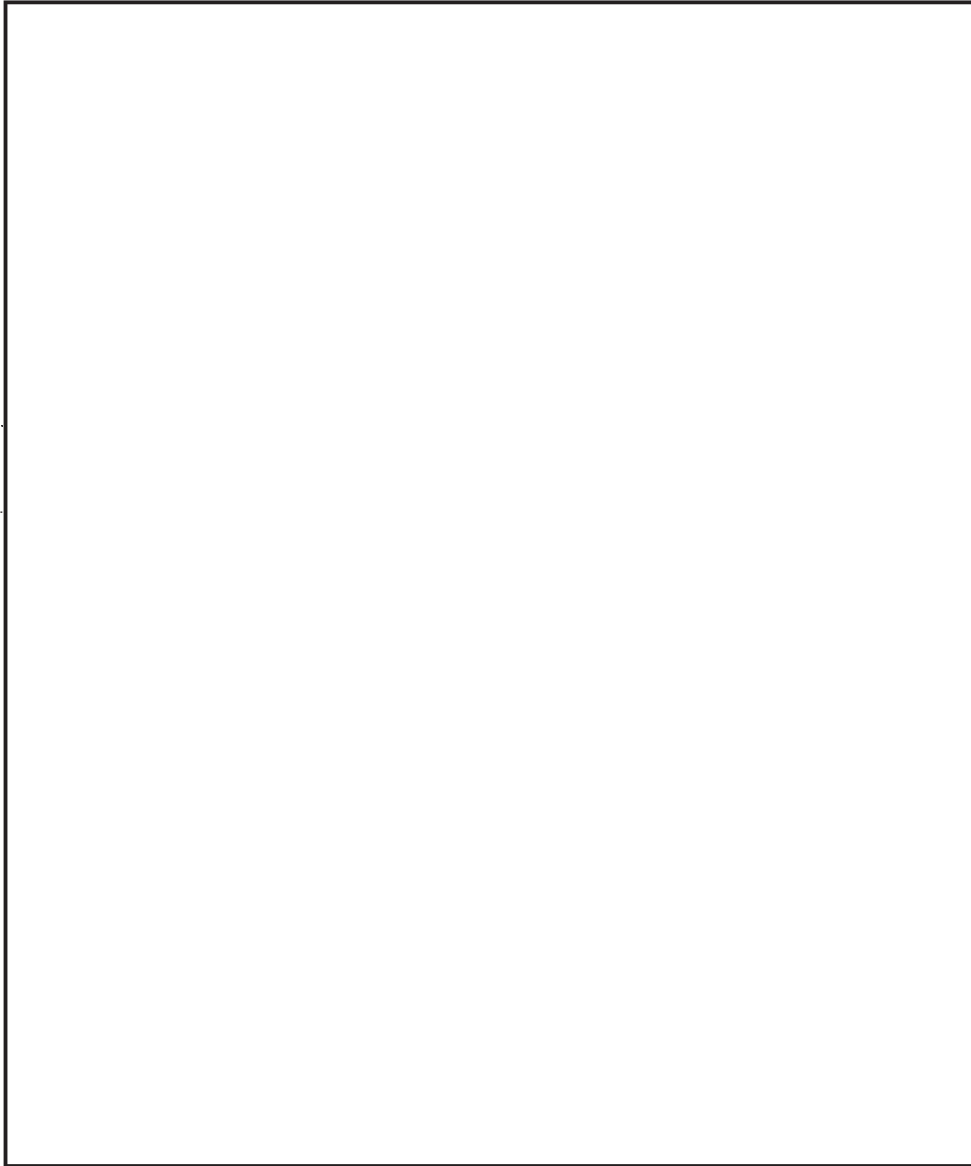
In the field of Communications Security our research effort has several objectives. First, it is directed at getting equipments of ever increasing reliability, simplicity of maintenance, and of the lowest practicable cost and weight. We use the latest and the most reliable components and the best and most modern electronics techniques. Secondly, to meet the user requirements we are developing equipments to provide communications security for the rapidly expanding communications needs of the United States. These include both conventional communications, e.g., voice and printer, but also somewhat more exotic requirements. For example, communications from the space satellites that must communicate information to the ground stations without the danger of unauthorized exploitation. Thirdly, our effort is aimed at the investigation of techniques which can counter and suppress the harmful short-range radiation I mentioned earlier in my speech. Fourthly, our work is also looking to tomorrow when we anticipate that the cryptanalyst with newer and more powerful analytic equipment five to ten years from now might be able to jeopardize some of the systems in use today. Therefore, we are developing tomorrow's systems in anticipation of what tomorrow's analytical equipments will be.

In the field of Signals Intelligence research and development I could perhaps explain part of what is done there by considering an actual example which would show the steps involved in the detection,

~~TOP SECRET DINA~~

~~TOP SECRET DINAR~~

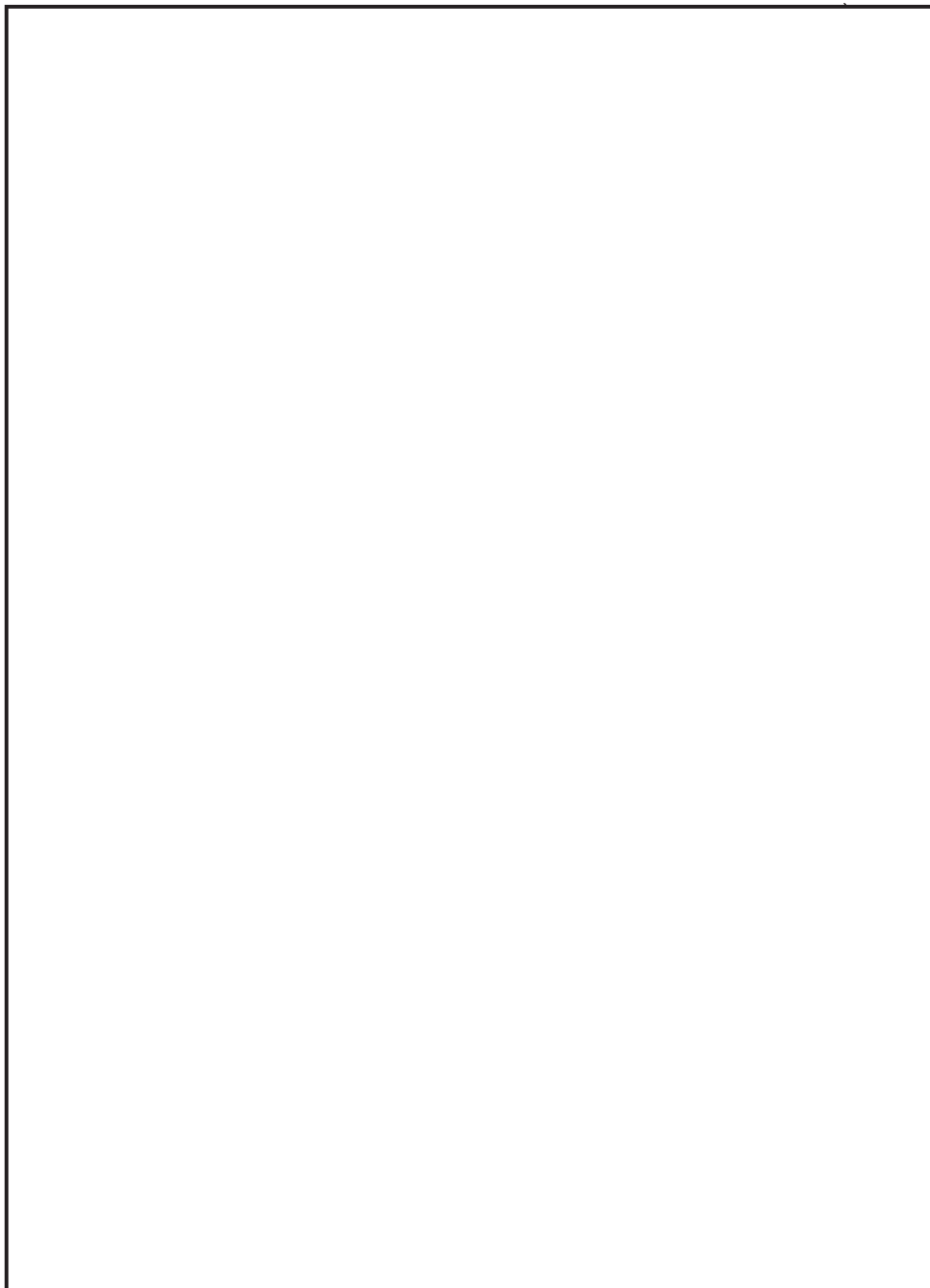
the collection, the analysis, and finally the exploitation of a new signal -



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

There are a number of other research and development areas of interest which would warrant mentioning except that shortage of time clearly makes this impossible. I note, however, a very deliberate research and development effort to develop the equipment and the techniques for tomorrow's problems. A perfect example of this approach is equipment called LIGHTNING which ultimately will provide computers capable of operating at up to 1,000 times the speed and with 1,000 times the capacity and power of today's equipments.

I conclude this discussion of research and development by noting that the National Security Agency Research and Development Office acts effectively as a member of the Secretary of Defense's Research and Engineering Organization to evaluate for him and to comment on all Service research and development programs related to the COMSEC and SIGINT missions. In this area as in others I have noted the National Security Agency works closely with the Service Cryptologic Agencies and with the Service Research Laboratories in the technical fulfillment of this responsibility.

Now to consider briefly the personnel and budgetary support which is given the National Security Agency and the Service Cryptologic Agencies in order to carry out the responsibilities that I have discussed up to this point. I have here a chart which gives an accurate picture of the military and civilian personnel resources of the National Security Agency, the Army

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

Security Agency, the Navy Security Group, and the Air Force Security Service. The military personnel include not only the operators who man the positions and the military analysts who man the field processing centers and the National Security Agency, but likewise include the cooks, truck drivers, and the maintenance men who are necessary and are used in the field to keep this equipment operating.

This chart shows the dollars that are funded for by the Service Cryptologic Agencies and justified by the National Security Agency in its annual presentation of the Combined Cryptologic Budget to the Department of Defense Comptroller and the Bureau of the Budget. Not included in this chart is any of the money involved in the payment of military salaries or military expenses such as change of station, retirement, etc. It is estimated that that cost for all the military personnel involved in COMSEC and SIGINT operations totals between [redacted]

(b)(1)
(b)(3)-P.L. 86-36

[redacted] dollars a year. This figure is not included in this chart because money for military pay is justified by each Service for all its personnel at one time and the Service Cryptologic Agencies do not fund for nor defend these monies. You will note that the cost of the National Security Agency SIGINT mission is about [redacted] dollars, the COMSEC mission about [redacted] the Research and Development mission about [redacted]. This chart does include the pay of all civilian personnel and you will note the total direct cost of cryptologic operations is about [redacted] dollars. This other missions column includes money that the Service

(b)(1)
(b)(3)-P.L. 86-36

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

Cryptologic Agencies must justify, fund, and defend but represents missions which do not come under the operational and technical control of the Director, National Security Agency. Such things include, for example, the Armed Forces Courier system of the Army Security Agency, the Registered Publications Issuing Office of the Navy Security Group, and various items of that sort.

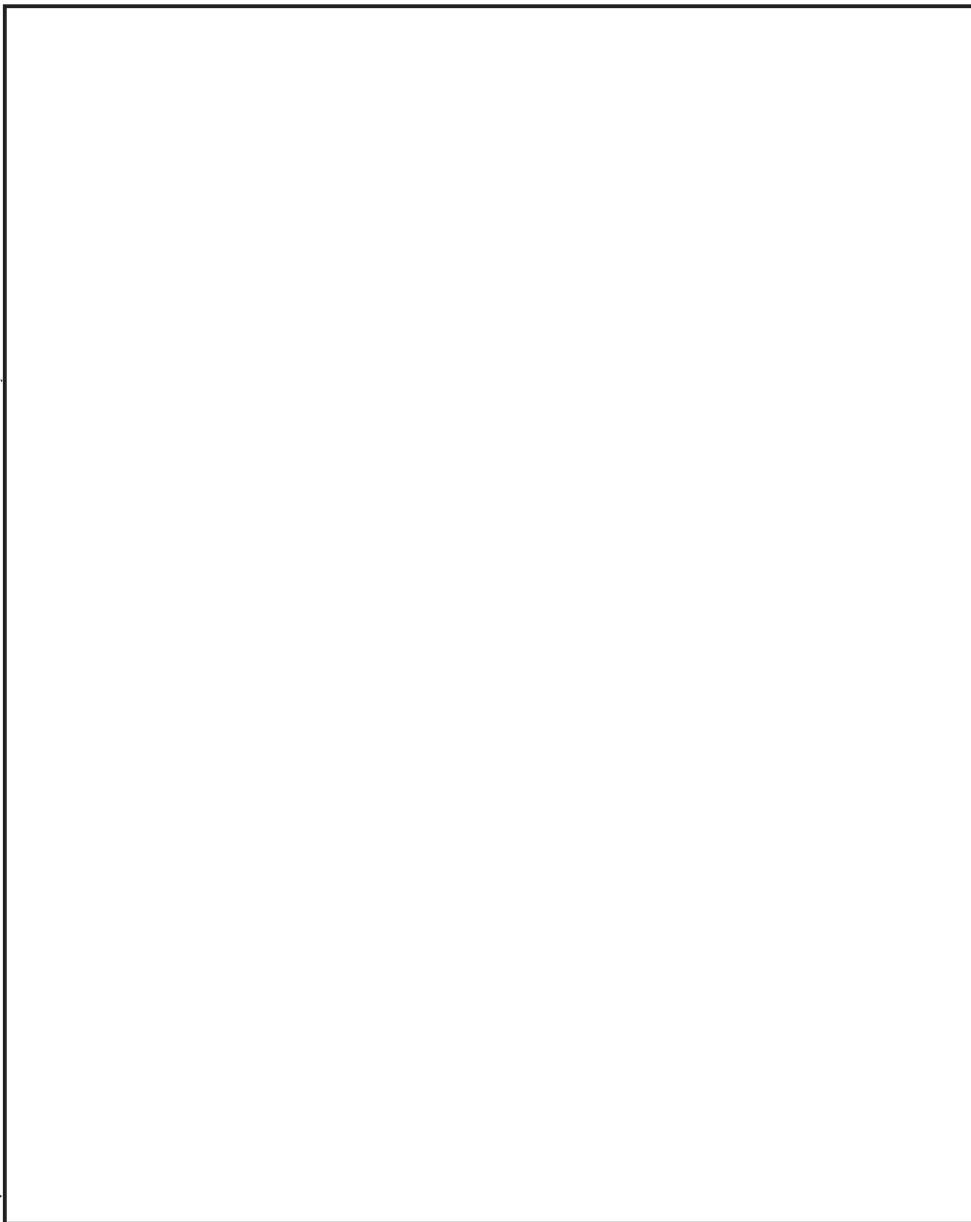
At this point, I think it would be appropriate to take a look at some of the recent outstanding successes of the Communications Security and Signals Intelligence operations. First, as I noted before the United States communications are capable of being completely secure if operating instructions are followed and money is made available to purchase the cryptographic equipment. Such secure equipment is available to meet almost any requirement of the Armed Services or the Civilian Agencies. The National Security Agency provides the necessary keying materials, evaluations, and operating procedures.

In the field of Signals Intelligence I will make a deliberate attempt to select certain signals intelligence highlights from the past few years. First I should like to note our effort and success in the late '40s up to the middle '50s in producing information

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~TOP SECRET DINAR~~

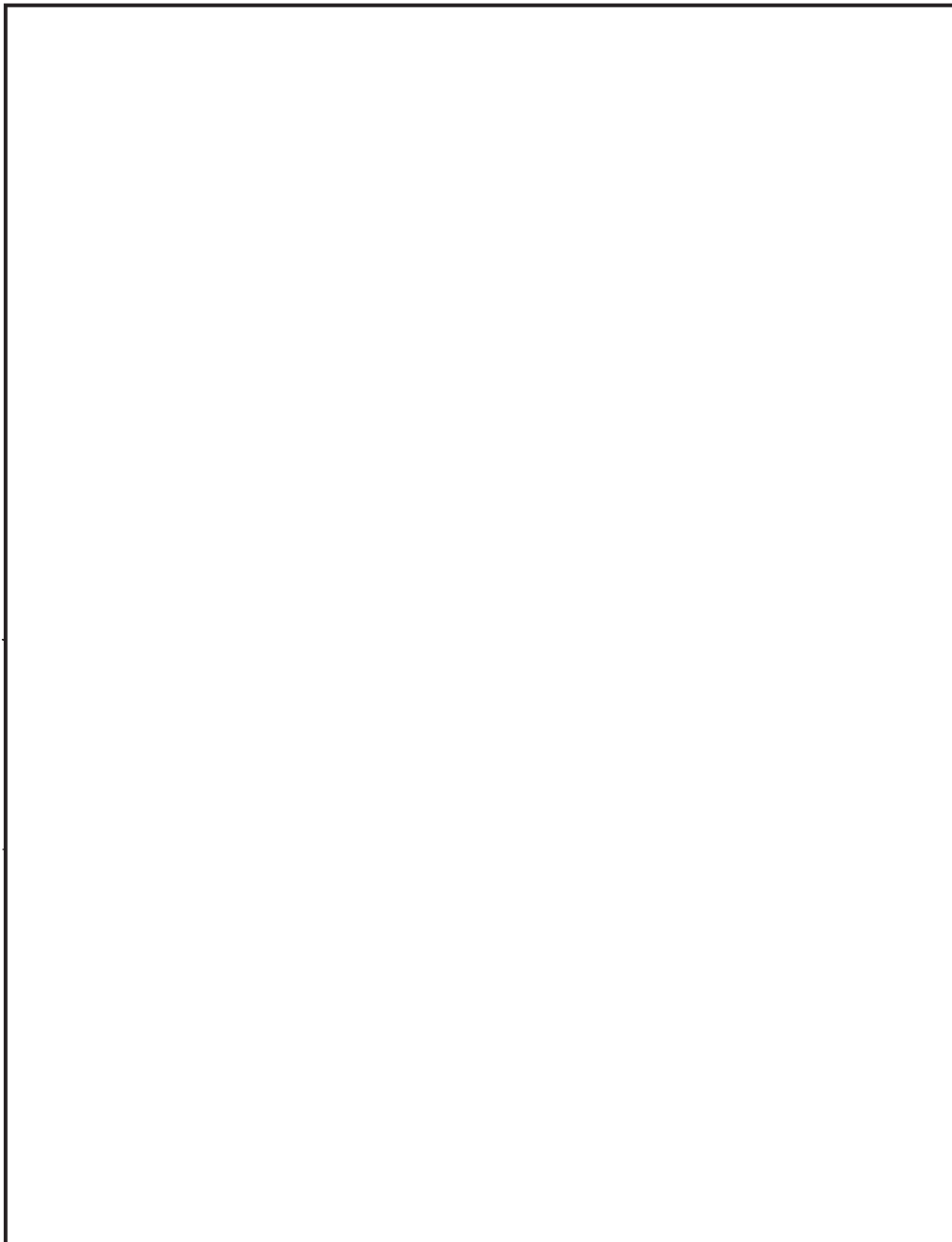
~~TOP SECRET DINAR~~



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

The National Security Agency

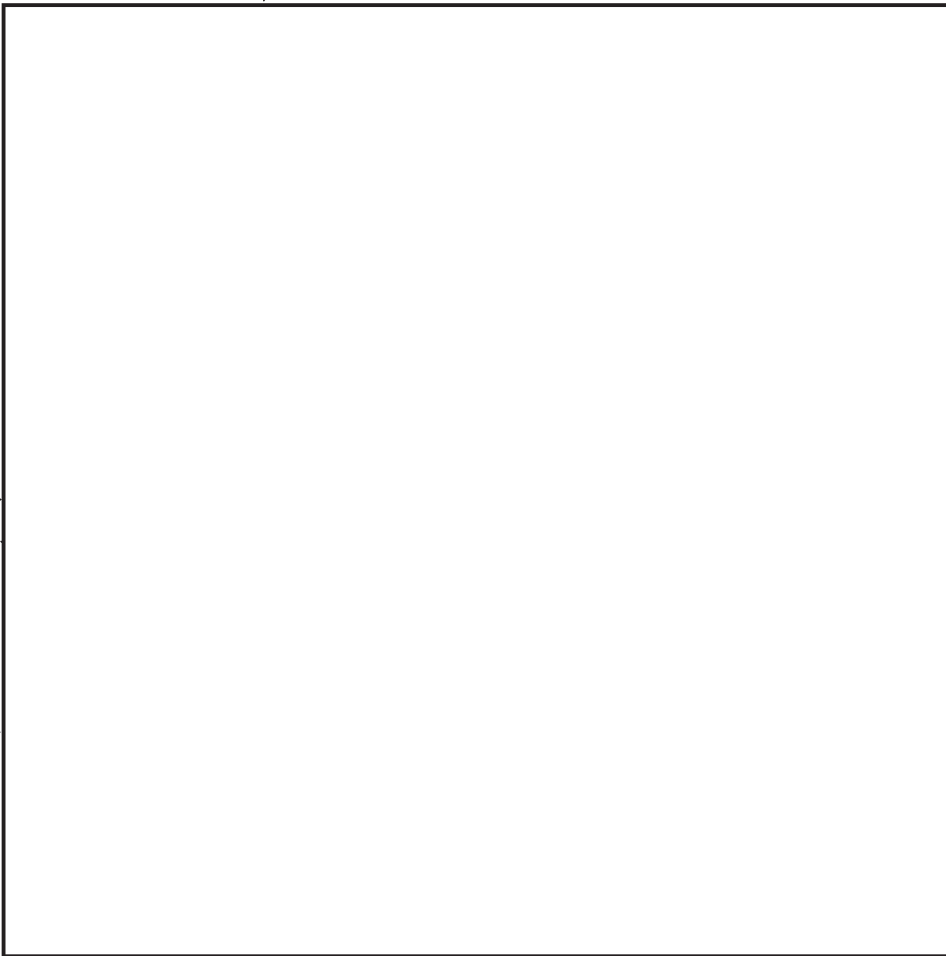
is responsible not only for developing this information but also for its timely delivery to the highest intelligence and policy levels of the United States Government.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~

So far I have spoken largely about the present or the immediate past. In conclusion I should like to consider briefly what the future holds. There is a growth in the number and the complexity of signals available for intercept from our past conventional sources and users.



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36

~~TOP SECRET DINAR~~

~~TOP SECRET DINAR~~



(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36


~~TOP SECRET DINAR~~

~~TOP SECRET DIN~~

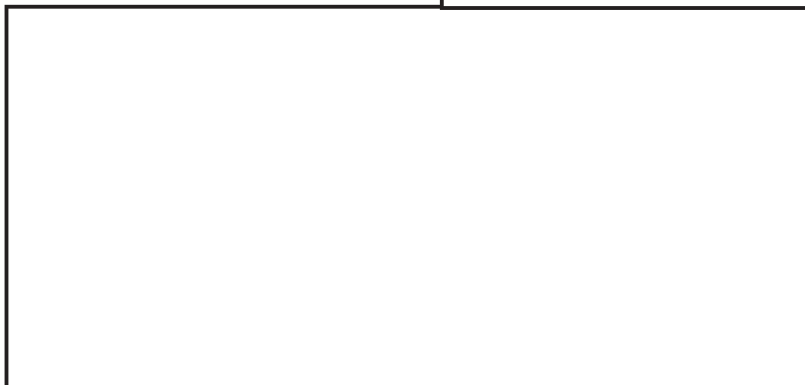
(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36



As evidence of its potential value to your Mr. McNamara I quote from an October JCS Memorandum for the Secretary of Defense in which the Chiefs remarked:

"4. The Joint Chiefs of Staff have been impressed with the service which the cryptologic agencies have rendered during the past year to the decision-making mechanism of the Department of Defense and our government in general. Especially valuable has been the COMINT provided on 

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 403
(b) (3)-P.L. 86-36



"5. In brief, the Joint Chiefs of Staff continue to rely heavily upon the informational base provided by COMINT and ELINT in the formulation of their advice." (J.C.S. 2010/161)

~~TOP SECRET DIN~~